

Unforgeable Noise-Tolerant Quantum Tokens

F. Pastawski^{1*}, N. Y. Yao², L. Jiang³, M. D. Lukin², J. I. Cirac¹

¹*Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, Garching, D-85748, Germany*

²*Physics Department, Harvard University, Cambridge, MA 02138 and*

³*Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125**

(Dated: November 21, 2012)

The realization of devices which harness the laws of quantum mechanics represents an exciting challenge at the interface of modern technology and fundamental science[1, 2]. An exemplary paragon of the power of such quantum primitives is the concept of “quantum money” [3]. A dishonest holder of a quantum bank-note will invariably fail in any forging attempts; indeed, under assumptions of ideal measurements and decoherence-free memories such security is guaranteed by the no-cloning theorem [4]. In any practical situation, however, noise, decoherence and operational imperfections abound. Thus, the development of secure “quantum money”-type primitives capable of tolerating realistic infidelities is of both practical and fundamental importance. Here, we propose a novel class of such protocols and demonstrate their tolerance to noise; moreover, we prove their rigorous security by determining tight fidelity thresholds. Our proposed protocols require only the ability to prepare, store and measure single qubit quantum memories, making their experimental realization accessible with current technologies [5–7].

Recent extensions to Wiesner’s original “quantum money” protocol [3] have garnered significant interest [8–11]. One particular extension enables the authentication of quantum tokens via classical public communication with a trusted verifier [12]. However, to tolerate noise, the verification process must condone a certain finite fraction of qubit failures; naturally, such a relaxation of the verification process enhances the ability for a dishonest user to forge quantum tokens. It is exactly this interplay which we, here, seek to address, by focusing on a class of “quantum token”-protocols which involve either direct physical or classical communication verification of qubit memories.

Our approach to quantum tokens extends the original quantum money primitive[3] by ensuring tolerance to finite errors associated with encoding, storage and decoding of individual qubits. We denote the tokens within our first primitive as quantum tickets (qtickets); each qticket is issued by the mint and consists of a unique serial number and N component quantum states, $\rho = \bigotimes_i \rho_i$, where each ρ_i is drawn uniformly at random from the

set, $\tilde{Q} = \{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle, |0\rangle, |1\rangle\}$, of polarization eigenstates of the Pauli spin operators. The mint secretly stores a classical description of ρ , distributed only among trusted verifiers. In order to redeem a qticket, the holder physically deposits it with a trusted verifier, who measures the qubits in the relevant basis. This verifier then requires a minimum fraction, F_{tol} , of correct outcomes in order to authenticate the qticket; following validation, the only information returned by the verifier is whether the qticket has been accepted or rejected.

The soundness of a qticket, e.g. the probability that an honest user is successfully verified, depends crucially on the experimental fidelities associated with single qubit encoding, storage and decoding. Thus, for a given qubit ρ_i , we define the map, M_i , which characterizes the overall fidelity, beginning with the mint’s encoding and ending with the verifier’s validation; the average channel fidelity[13] is then given by, $F_i = 1/|\tilde{Q}| \sum_{\rho_i} \text{Tr}[\rho_i M_i(\rho_i)]$. With this definition, the verification probability of an honest user is,

$$p_h = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}} M(\rho)] \geq 1 - e^{-ND(F_{\text{exp}} \| F_{\text{tol}})}, \quad (1)$$

where $Q = \tilde{Q}^{\otimes N}$, P_{acc} represents the projector onto the subspace of valid qtickets, $M = \bigotimes_i M_i$, $F_{\text{exp}} = 1/N \sum_i F_i$ is the average experimental fidelity, and D , the relative entropy, characterizes the distinguishability of two distributions (see Methods for details). Crucially, so long as the average experimental fidelity associated with single qubit processes is greater than the tolerance fidelity, an honest user is exponentially likely to be verified.

To determine a tight security threshold, we consider the counterfeiting of a single qticket. For a given tolerance fidelity (F_{tol}) set by the verifiers, a qticket is only accepted if at least $F_{\text{tol}}N$ qubits are validated. In the event that a dishonest user attempts to generate two qtickets from a single valid original, *each* must contain a minimum of $F_{\text{tol}}N$ valid qubits to be authenticated. As depicted in Fig. 1a., in order for each counterfeit qticket to contain $F_{\text{tol}}N$ valid qubits, a *minimum* of $(2F_{\text{tol}} - 1)N$ qubits must have been perfectly cloned. Thus, for a set tolerance fidelity, in order for a dishonest user to succeed, he or she must be able to emulate a qubit cloning fidelity of at least $2F_{\text{tol}} - 1$. Crucially, so long as this fidelity is above that achievable for optimal qubit cloning (2/3)

*Electronic address: fernando.pastawski@mpq.mpg.de

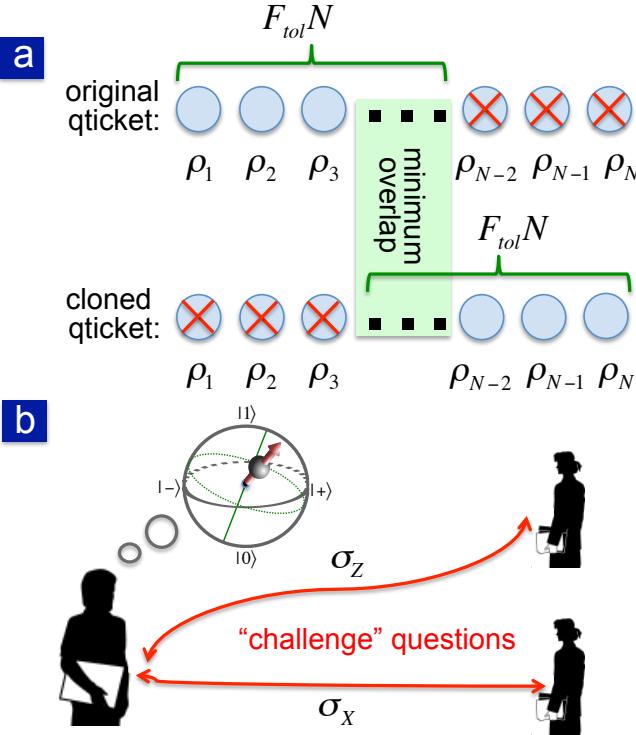


FIG. 1: a) Depicts the pigeonhole type argument which is utilized in the proof of qticket soundness. For a tolerance fidelity F_{tol} , a qticket is only successfully authenticated if it contains at least $F_{\text{tol}}N$ valid qubits. However, for two counterfeit qtickets, not all valid qubits must coincide. The minimum number of perfectly cloned qubits enabling both qtickets to be accepted is, $(2F_{\text{tol}} - 1)N$. b) Depicts the quantum retrieval type situation envisioned for cv-qtickets. For two verifiers asking complementary “challenge” questions, the optimal strategy is for the user to measure in an intermediate basis. Such a strategy saturates the tolerance threshold, $F_{\text{tol}}^{\text{cv}} = \frac{1+1/\sqrt{2}}{2}$.

[14], a dishonest user is exponentially unlikely to succeed,

$$p_{\text{d}} = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr} [P_{\text{acc}}^{\otimes 2} T(\rho)] \leq e^{-ND(2F_{\text{tol}}-1)^{2/3}}, \quad (2)$$

where T represents any completely positive trace preserving qticket counterfeiting map. To ensure $2F_{\text{tol}}-1 > 2/3$, the tolerance fidelity must be greater than $5/6$, which is precisely the average fidelity of copies produced by an optimal qubit cloning map [14]. In certain cases, an adversary may be able to sequentially engage in multiple verification rounds; however, the probability of successfully validating counterfeited qtickets grows at most quadratically in the number of such rounds, and hence, the likelihood of successful counterfeiting can remain exponentially small even for polynomially large numbers of verifications.

Our previous discussion of qtickets assumed that such tokens are physically transferable to trusted verifiers (e.g. concert tickets); however, in many situations, this as-

sumption of physical deposition, may either be impossible or undesirable. Recently, it has been shown [12] that it remains possible, even remotely, for a holder to prove the validity of a token by responding to a set of “challenge” questions; these questions can only be successfully answered by measuring an authentic token. The core behind this approach is to ensure that the “challenge” questions reveal no additional information about the quantum state of the token.

We now discuss a specific realization of such an approach, the classical verification quantum ticket (cv-qticket), and demonstrate its robustness against noise and operational imperfections. In contrast to the case of bare qtickets, a cv-qticket holder will be expected to answer “challenge” questions and hence to measure qubits himself. One might imagine that the ability to participate in multiple remote verifications simultaneously could offer a dishonest user an additional advantage over the bare qticket case; in particular, certain measurement strategies may yield an increased likelihood for multiple successful authentications.

One example of a cv-qticket framework, is to utilize a set of eight possible two-qubit product states with each qubit prepared along either X or Z (note that a single qubit framework is also possible):

$$\{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |-,0\rangle, |+,1\rangle, |-,1\rangle\}.$$

We then envision each cv-qticket to consist of n blocks, each containing r qubit pairs, and thus, a total of $n \times r \times 2$ qubits; as before, each of the qubit pairs is chosen uniformly at random from the allowed set above. A “challenge” question consists of randomly asking the holder to measure each block (of qubits) along either the X or Z basis; naturally, as depicted in Table 1, a valid qubit pair (within a block) is one in which the holder correctly answers the state for the particular qubit (within the pair) which was prepared along the questioned basis. For a given tolerance threshold, an overall answer will only be deemed correct if at least $F_{\text{tol}}^{\text{cv}}r$ qubits within each of the n blocks are found valid. By analogy to the qticket case, honest users are exponentially likely to be verified so long as $F_{\text{exp}} > F_{\text{tol}}^{\text{cv}}$; in particular, since there now exist n blocks of qubits, each of which can be thought of as an individual qticket (with r qubits),

$$p_{\text{h}}^{\text{cv}} \geq \left(1 - e^{-rD(F_{\text{exp}} \| F_{\text{tol}}^{\text{cv}})}\right)^n. \quad (3)$$

The proof of cv-qticket security is based upon a generalized formalism of quantum retrieval games [12, 15], in combination with a generalized Chernoff-Hoeffding bound [16] (details in Supplementary Information). So long as $F_{\text{tol}}^{\text{cv}} > \frac{1+1/\sqrt{2}}{2}$, a dishonest user is exponentially unlikely to be authenticated by two independent verifiers. For two complementary “challenge” questions, one finds that on average, no more than $1 + 1/\sqrt{2} \approx 1.707$ can be answered correctly. Interestingly, the threshold $F_{\text{tol}}^{\text{cv}}$ corresponds exactly to that achievable by either covariant

Prepare	$ -, 0\rangle$ $ 0, +\rangle$ $ 1, +\rangle$ $ 0, +\rangle$	$ 0, +\rangle$ $ +, 1\rangle$ $ -, 0\rangle$ $ 1, +\rangle$
B:Ask	Z	X
H:Ans.	0, 0 0, 1 1, 1 0, 1	$-$, $+$ $+$, $-$ $-$, $+$ $+$, $-$
Correct	\checkmark \checkmark \checkmark \checkmark	\checkmark \checkmark \checkmark \times
Block		\checkmark
B:Res.		Verified

TABLE I: Verification of a single cv-qticket. Here, we consider a cv-qticket with $n = 4$ and $r = 2$, totaling 8 qubit pairs and $F_{\text{tol}} = 3/4$ (for illustrative purposes only). The prepared qubit-pairs are chosen at random, as are the bank's requested measurement bases (for each block). The holder's answer has at most, a single error per block, which according to, $F_{\text{tol}} = 3/4$, is allowed. Secure cv-qtickets require $F_{\text{tol}} > 1/2 + 1/\sqrt{8}$ and a larger number of constituent qubits.

qubit cloning[17] or by measurement in an intermediate basis (Fig. 1b.), suggesting that both such strategies may be optimal [2]. Similar to the qticket case, one finds that a dishonest user is exponentially likely to fail,

$$p_d^{\text{cv}} \leq \binom{v}{2}^2 \left(1/2 + e^{-rD(F_{\text{tol}}\parallel \frac{1+1/\sqrt{2}}{2})}\right)^n, \quad (4)$$

where v represents the number of repeated verification attempts (for details see Supplementary Information). Moreover, so long as two verifiers agree to ask complementary “challenge” questions, participation in simultaneous verifications is unable to improve a dishonest user’s emulated fidelity. Thus, in the case of both qtickets and cv-qtickets, so long as the hierarchy of fidelities is such that: $F_{\text{dishonest}} < F_{\text{tol}} < F_{\text{exp}}$, it is possible to prove both soundness and security of each protocol.

Next, we consider applications of the above primitives to practically relevant protocols. For instance, one might imagine a composite cv-qticket which allows for multiple verification rounds while also ensuring that the token cannot be split into two independently valid sub-parts [12]. Such a construction may be used to create a quantum-protected credit card. Indeed, the classical communication which takes place with the issuer (bank) to verify the cv-qticket (via “challenge” questions) may be intentionally publicized to a merchant who needs to be convinced of the card’s validity. By contrast to modern credit card implementations, such a quantum credit card would be unforgeable and hence immune to fraudulent charges (Fig. 2a).

An alternate advantage offered by the qticket framework is evinced in the case where verifiers may not possess a secure communication channel with each other. Consider for example, a dishonest user who seeks to copy multiple concert tickets, enabling his friends to enter at different checkpoint gates. A classical solution would involve gate verifiers communicating amongst one another to ensure that each ticket serial number is only allowed entry a single time; however, as shown in Fig. 2b., such a safeguard can be overcome in the event that communication has been severed. By contrast, a concert ticket

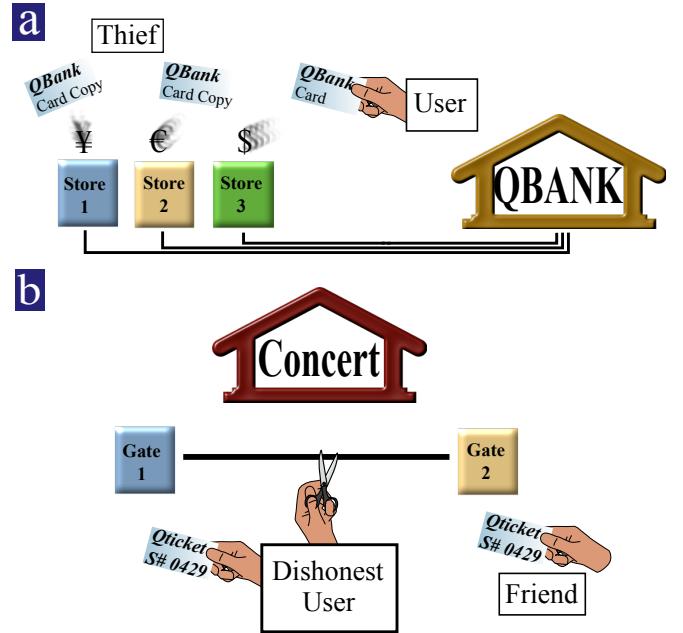


FIG. 2: a) Depicts the possibility of using the cv-qticket framework to implement a quantum-protected credit card. Unlike its classical counterpart, the quantum credit card would naturally be unforgeable; this prevents thieves from being able to simply copy credit card information and perform remote purchases. b) Depicts a dishonest user who attempts to copy a concert qticket (e.g. same serial number), enabling his friend to enter at an alternate checkpoint gate. Naively, each verifier can communicate with one another to prevent such abusive ticket cloning. However, such a safeguard can be overcome in the event that the communication among verifiers is either unsecured, unavailable or severed (possibly by the dishonest user himself). The qticket is exempt from this type of attack since security is guaranteed even in the case of isolated verifiers.

based upon the proposed qticket primitive would be automatically secure against such a scenario; indeed, the security of qtickets is guaranteed even when verifiers are assumed to be isolated. Such isolation may be especially useful for applications involving quantum identification tokens, where multiple verifiers may exist who are either unable or unwilling to communicate with one another.

While quantum primitives have been the subject of tremendous theoretical interest, their practical realization demands robustness in the face of realistic imperfections. Our above analysis demonstrates that such noise tolerance can be achieved for certain classes of unforgeable quantum tokens. Moreover, the derived tolerance thresholds are remarkably mild and suggest that proof of principle experiments are currently accessible in systems ranging from trapped ions [5, 18] and superconducting devices [6, 19] to solid-state spins [7, 20–22]. In particular, recent advances on single nuclear spins situated in a compact room-temperature solid, have demonstrated that ultra-long storage times can be attained in combination with high fidelity initialization and readout [7];

such advances suggest that quantum devices based upon single qubit quantum memories may be both practical and realistically feasible.

While our analysis has focused on describing a primitive based upon single tokens, natural extensions to the case of multiple identical quantum tokens open up the possibility of even more novel applications. In particular, as detailed in the Supplementary Information, it is possible to extend our threshold results to the case where c identical copies of the quantum token are issued. In this case, to ensure that the production of $c+1$ valid tokens is exponentially improbable, the required threshold fidelity must be greater than $1 - \frac{1}{(c+1)(c+2)}$. The existence of such multiple identical tokens can provide a certain degree of anonymity for users and could be employed in primitives such as quantum voting. A crucial question that remains is whether a rigorous proof of anonymity can be obtained in a noisy environment. Furthermore, our proposed quantum tokens can also be seen as a basic noise tolerant building block for implementing more advanced application schemes; such schemes can range from novel implementations of quantum key distribution [2, 23–25] based upon physical qubit transport to complex one-time-entry identification cards. Beyond these specific applications, a number of scientific avenues can be explored, including for example, understanding whether an interplay between computational assumptions and quantum memories can yield fundamentally new approaches to encryption.

Methods

Proof of Quantum Ticket Soundness— To demonstrate the soundness and security of qtickets, we employ the framework of a Chernoff Bound, which characterizes the central limiting behavior of a set of independent random variables; in particular, it provides exponentially decreasing bounds on tail distributions of their sums. Here, we state a generalization of this bound [16],

Theorem: Generalized Chernoff-Hoeffding bound
Let X_1, \dots, X_n be Boolean $\{0, 1\}$ random variables, such that for some δ_i and every $S \subseteq \{1, \dots, n\}$, it holds that $\Pr[\bigwedge_{i \in S} X_i] \leq \prod_{i \in S} \delta_i$. Then

$$\Pr\left[\sum_{i=1}^n X_i \geq \gamma n\right] \leq e^{-nD(\gamma\|\delta)}$$

with $\delta := n^{-1} \sum_{i=1}^n \delta_i$ and for any γ s.t. $\delta \leq \gamma \leq 1$.

$D(p\|q) = p \ln \frac{p}{q} + (1-p) \ln \frac{1-p}{1-q}$ characterizes the distinguishability of two binary probability distributions, where $\Pr(X=1) = p$ for the first distribution and $\Pr(X=1) = q$ for the second. To establish the soundness of qtickets, we now define the “acceptor”, P_{acc}^ρ , which projects a pure N qubit product state onto the subspace

of valid qtickets. As expected, the size of this subspace will depend on the verifiers tolerance fidelity, F_{tol} .

Definition: Acceptance Projector

Given $\rho = \bigotimes_{i=1}^N \rho_i$ and a security parameter $0 \leq F_{\text{tol}} \leq 1$, the acceptance projector is given by

$$P_{\text{acc}}^\rho = \sum_{\vec{b}: |\vec{b}|_1 \geq F_{\text{tol}}N} \bigotimes_{i=1}^N (b_i \rho_i + \bar{b}_i \rho_i^\perp).$$

$\vec{b} \in \{0, 1\}^N$ is a length N , boolean string with $|\vec{b}|_1 = \sum_{i=1}^N b_i$, $\bar{b}_i = 1 - b_i$, and $\rho_i^\perp = \mathbb{1} - \rho_i$. Intuitively, $|\vec{b}|_1$ can be thought of as a Hamming weight since it characterizes the number of non-zero entries of the string. The sum is over all strings which have at least $F_{\text{tol}}N$ entries which are 1; thus, the definition of \vec{b} naturally enforces the projection onto the set of valid qticket states. We now recall the qubit map M_i which characterizes the overall fidelity, F_i , of encoding, storage and decoding. We define $F_{\text{exp}} = 1/N \sum_i F_i$ to be the average achievable experimental fidelity. This brings us to the statement of qticket soundness.

Theorem: Soundness of a Quantum Ticket

For $F_{\text{exp}} > F_{\text{tol}}$, an honest holder successfully redeem a qticket with probability

$$p_v \geq 1 - e^{-ND(F_{\text{tol}}\|F_{\text{exp}})}.$$

Proof. Consider a vector composed of boolean random variables, $\vec{X} = (X_1, \dots, X_N)$, with a joint probability distribution given by

$$\begin{aligned} \Pr[\vec{X} = \vec{b}] &= \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr} \left[M(\rho) \bigotimes_{i=1}^N (b_i \rho_i + \bar{b}_i \rho_i^\perp) \right] \\ &= \prod_{i=1}^N \frac{1}{6} \sum_{\rho_i \in \tilde{Q}} \text{Tr} [M_i(\rho_i)(b_i \rho_i + \bar{b}_i \rho_i^\perp)] \end{aligned}$$

As evidenced, we can consider X_i to be independent boolean random variables with probability $\Pr[X_i] = F_i$. Moreover, a simple calculation reveals that Eq. 1 of the main text can be recast as, $\frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^\rho M(\rho)] = \Pr[\sum_{i=1}^N X_i \geq F_{\text{tol}}N]$. Application of the Chernoff bound yields the desired result. ■

The security proof for qtickets, detailed in the supplementary information, follows in a similar fashion; it requires the generalized Chernoff-Hoeffding bound to rigorously deal with arbitrary counterfeiting attacks, which may in principle generate correlations between qticket components.

Acknowledgements

We thank Y. Chu, C. R. Laumann and S. D. Bennett for insights and discussions. This work was supported

in part by the DFG (SFB 631), the QCCC elite network Bayern, the EU project MALICIA and Catalunya Caixa, the NSF, CUA, DOE (FG02-97ER25308), DARPA

(QuEST), MURI, Packard Foundation and the Sherman Fairchild Foundation.

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, New York, 2000), ISBN 0521635039, 9780521635035.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Reviews of Modern Physics* **74**, 145 (2002), URL <http://link.aps.org/doi/10.1103/RevModPhys.74.145>.

[3] S. Wiesner, ACM SIGACT News **15**, 78 (1983), ISSN 01635700, URL <http://dl.acm.org/citation.cfm?id=1008920>.

[4] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982), URL <http://dx.doi.org/10.1038/299802a0>.

[5] D. B. Hume, T. Rosenband, and D. J. Wineland, *Phys. Rev. Lett.* **99**, 120502 (2007).

[6] G. Wordin, *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **361**, 1323 (2003), URL <http://rsta.royalsocietypublishing.org/content/361/1808/1323.abstract>.

[7] P. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, et al. (2011).

[8] S. Aaronson, in *24th Annual IEEE Conference on Computational Complexity, 2009*. (IEEE, 2009), pp. 229–242.

[9] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor, 0912.3825 (2009), URL <http://arxiv.org/abs/0912.3825>.

[10] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, D. Nagaj, and P. Shor, *Physical Review Letters* **105**, 190503 (2010), URL <http://link.aps.org/doi/10.1103/PhysRevLett.105.190503>.

[11] A. Lutomirski, 1107.0321 (2011), URL <http://arxiv.org/abs/1107.0321>.

[12] D. Gavinsky, arXiv:1109.0372 (2011), URL <http://arxiv.org/abs/1109.0372>.

[13] M. A. Nielsen, *Physics Letters A* **303**, 249 (2002), ISSN 0375-9601, URL <http://www.sciencedirect.com/science/article/B6TVM-46W1DCY-6/2/40565f4089f0646a7525fabf4ccc44c5>.

[14] R. F. Werner, *Physical Review A* **58**, 1827 (1998), URL <http://link.aps.org/doi/10.1103/PhysRevA.58.1827>.

[15] G. Gutoski and J. Watrous, in *Proceedings of the ninth annual ACM symposium on Theory of computing* (ACM, New York, NY, USA, 2007), STOC '07, p. 565?574, ISBN 978-1-59593-631-8, URL <http://doi.acm.org/10.1145/1250790.1250873>.

[16] R. Impagliazzo and V. Kabanets, *Tech. Rep.* 072 (2010), URL <http://eccc.hpi-web.de/report/2010/072/>.

[17] D. Bruss, M. Cinchetti, G. Mauro D'Ariano, and C. Macchiavello, *Physical Review A* **62**, 012302 (2000), URL <http://link.aps.org/doi/10.1103/PhysRevA.62.012302>.

[18] C. Langer, R. Ozeri, J. D. Jost, J. Chiaverini, B. DeMarco, A. Ben-Kish, R. B. Blakestad, J. Britton, D. B. Hume, W. M. Itano, et al., *Phys. Rev. Lett.* **95**, 060502 (2005).

[19] S. Gladchenko, D. Olaya, E. Dupont-Ferrier, B. Doucot, L. B. Ioffe, and M. E. Gershenson, *Nat Phys* **5**, 48 (2009), ISSN 1745-2473, URL <http://dx.doi.org/10.1038/nphys1151>.

[20] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin, *Science* **316**, 1312 (2007), URL <http://www.sciencemag.org/cgi/content/abstract/316/5829/1312>.

[21] J. J. L. Morton, A. M. Tyryshkin, R. M. Brown, S. Shankar, B. W. Lovett, A. Ardavan, T. Schenkel, E. E. Haller, J. W. Ager, and S. A. Lyon, *Nature* **455**, 1085 (2008), ISSN 0028-0836, URL <http://dx.doi.org/10.1038/nature07295>.

[22] G. Balasubramanian, P. Neumann, D. Twitchen, M. Markham, R. Kolesov, N. Mizuuchi, J. Isoya, J. Achard, J. Beck, J. Tissler, et al., *Nat Mater* **8**, 383 (2009), ISSN 1476-1122, URL <http://dx.doi.org/10.1038/nmat2420>.

[23] C. H. Bennet and G. Brassard, International Conference on Computers, Systems & Signal Processing (1984), bangalore, India.

[24] D. Gottesman and H. Lo, *IEEE Transactions on Information Theory* **49**, 457 (2003), ISSN 0018-9448.

[25] V. Scarani and R. Renner, *Physical Review Letters* **100**, 200501 (2008), URL <http://link.aps.org/doi/10.1103/PhysRevLett.100.200501>.

SUPPLEMENTARY INFORMATION

Unforgeable Noise-Tolerant Quantum Tokens

F. Pastawski¹, N. Y. Yao², L. Jiang³, M. D. Lukin², J. I. Cirac¹

¹*Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, Garching, D-85748, Germany*

²*Physics Department, Harvard University, Cambridge, MA 02138 and*

³*Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125*

(Dated: November 21, 2012)

S.1. NOTATION AND EXTERNAL RESULTS

The following definitions and external results will be used extensively throughout the proofs and are included here to provide a self-contained presentation.

Definition 1 A quantum state t -design is a probability distribution over pure quantum states $(p_i, |\psi_i\rangle)$ such that

$$\sum_i p_i (|\psi_i\rangle\langle\psi_i|)^{\otimes t} = \int_{\text{Haar}} (|\psi\rangle\langle\psi|)^{\otimes t} d\psi.$$

In other words, a quantum state t -design duplicates the properties of the unique unitarily invariant Haar measure over quantum states for all polynomials up to degree t . We will use the set of states

$$\tilde{Q} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\} \quad (\text{S1})$$

with equal weights $p_i = 1/6$; this constitutes a quantum state 3-design over \mathcal{H}_2 [SI].

The average fidelity for a channel quantifies how well the channel preserves quantum states.

Definition 2 The Average fidelity of a map M is defined as

$$F(M) = \int_{\text{Haar}} \langle\psi | M(|\psi\rangle\langle\psi|) | \psi\rangle d\psi.$$

Note for example that the average fidelity of a map M is expressed as a Haar integral of a degree 2 polynomial expression in bras and kets and can thus be equated to a weighted average over a quantum state 2-design.

Throughout the text, boolean values $\mathcal{B} = \{\text{True}, \text{False}\}$ will be represented as $\text{True} := 1$, $\text{False} := 0$ and the negation $\bar{b} := 1 - b$. We will also use the variable \vec{b} to denote boolean strings (i.e. ordered sequences of values in $\{0, 1\}$) with $\text{len}(\vec{b})$ denoting the length or number of components of a sequence and $\text{tl}(\vec{b})$ denoting the string obtained from removing the last element from \vec{b} . We will denote by $\text{Pr}[e]$ the probability of an event e and $\text{Exp}[v]$ the expectation value of an expression v . Note that according to our convention, if the expression is a boolean formula they may be used interchangeably.

The relative entropy is a distinguishability measure between two probability distributions. It will be used extensively (particularly among binary or Bernoulli distributions) and appears in the definition of auxiliary results. Let $0 \leq p, q \leq 1$, by abuse of notation, we take $D(p\|q) = p \ln \frac{p}{q} + (1 -$

$p) \ln \frac{1-p}{1-q}$, the relative entropy between two Bernoulli probability distributions with respective parameters p and q . Note that this definition satisfies $D(p\|q) \geq 2(p - q)^2$.

The following generalization of the Chernoff-Hoeffding bound derived by Panconesi and Srinivasan [S2] provides the same thesis as a standard Chernoff bound while relaxing the hypothesis to allow dependent random variables.

Theorem 3 (Generalized Chernoff-Hoeffding bound) Let X_1, \dots, X_n be Boolean $\{0, 1\}$ random variables, such that for some δ_i and every $S \subseteq \{1, \dots, n\}$, it holds that $\text{Pr}[\bigwedge_{i \in S} X_i] \leq \prod_{i \in S} \delta_i$. Then

$$\text{Pr}\left[\sum_{i=1}^n X_i \geq \gamma n\right] \leq e^{-nD(\gamma\|\delta)}$$

with $\delta := n^{-1} \sum_{i=1}^n \delta_i$ and for any γ s.t. $\delta \leq \gamma \leq 1$.

A further generalization to real valued random variables will also be required. This is adapted to our purpose from theorem 3.3 of Impagliazzo and Kabanets [S3].

Theorem 4 Let X_1, \dots, X_n be real valued random variables, with each $X_i \in [0, 1]$. Suppose that there is a $0 \leq \delta \leq 1$ s.t., for every set $S \subseteq \{1, \dots, n\}$, $\text{Exp}[\prod_{i \in S} X_i] \leq \delta^{|S|}$ and γ s.t. $\delta \leq \gamma \leq 1$ and $\gamma n \in \mathbb{N}$. Then we have that $\text{Pr}[\sum_{i=1}^n X_i \geq \gamma n] \leq 2e^{-nD(\gamma\|\delta)}$.

S.2. QTICKETS

We first provide a rigorous definition of qtickets and how they are verified. We then proceed to our claims, and the soundness, security and tightness of our security bound (accompanied with respective proofs). Namely, we show that qtickets may be successfully redeemed by an honest holder achieving a sufficiently good storage fidelity. We then show that a dishonest holder will have a negligible chance of producing two qtickets which are accepted by verifiers from a single valid qticket, even after repeated verification attempts. Finally we show how a simple counterfeiting strategy has a high probability of producing two such qtickets if the verification tolerance is set below the threshold value. As an extension, we consider how our results generalize to producing multiple identical qtickets.

S.2.1. Definition of qtickets

Each qticket consists of a serial number s and an N component pure product state $\rho^{(s)} = \bigotimes_{i=1}^N \rho_i^{(s)}$. For each serial number s , qticket components $\rho_i^{(s)}$ are chosen uniformly at random from \tilde{Q} . This means qtickets $\rho^{(s)}$ are taken uniformly at random from the set $Q = \tilde{Q}^{\otimes N}$ (where by abuse of notation, the elements of Q are N component pure product states in $\mathcal{H}_Q = \mathcal{H}_2^N$, with components taken from \tilde{Q}). The verifiers store a database containing, for each s , a classical description of $\rho^{(s)}$ kept secret from ticket holders and the general public. In order to simplify notation, the serial number s associated to individual qtickets will be omitted from now on.

In order to use qtickets, they are transferred to a verification authority who can either accept or reject them. In both cases however, the qticket is not returned, only the binary outcome of verification. The qticket protocol is additionally parametrized by the fraction F_{tol} of qubits that a verification authority requires to be correct in order for verification to succeed. In order to verify a submitted qticket $\tilde{\rho}$, a full measurement will be performed in the product basis associated to the original qticket ρ and the number of correct outcomes is then counted. If more than at least $F_{\text{tol}}N$ are correct, the (possibly noisy) submitted qticket $\tilde{\rho}$ is accepted, otherwise, it is rejected.

For any pure product state $\rho = \bigotimes_{i=1}^N \rho_i$ we define a projector $P_{\text{acc}}^\rho \in \mathcal{L}(\mathcal{H}_Q)$ associated to the subspace of states that would be accepted if ρ were a qticket (i.e. states coinciding with ρ in at least a fraction F_{tol} of the qubits). The projector P_{acc}^ρ offers a more abstract interpretation and may be rigorously defined as

Definition 5 (Acceptance projector) *Given a pure N qubit product state $\rho = \bigotimes_{i=1}^N \rho_i$ and a security parameter $0 \leq F_{\text{tol}} \leq 1$, we define the acceptance projector*

$$P_{\text{acc}}^\rho = \sum_{\vec{b}: \sum b_i \geq F_{\text{tol}}N} \bigotimes_{i=1}^N (b_i \rho_i + \bar{b}_i \rho_i^\perp),$$

where $\vec{b} \in \{0, 1\}^N$ is a boolean string.

By abuse of notation, ρ_i and its orthogonal complement $\rho_i^\perp := \mathbb{1}_2 - \rho_i$ are used as rank 1 projectors in $\mathcal{L}(\mathcal{H}_2)$.

S.2.2. Soundness

The soundness result states that even under imperfect storage and readout fidelity, legitimate qtickets work well as long as the fidelity loss is not too severe. The completely positive trace preserving (CPTP) maps M_i will be assumed to represent the encoding, storage and readout of the i -th qubit component of the qticket. In this sense, the soundness statement takes place at the level of single qubits. This is necessarily the case, since legitimate qtickets are ruined if a significant fraction of the qubits fail in a correlated way. Given

$F_i = F(M_i)$, the average fidelity of the qubit map M_i , we define $F_{\text{exp}} := N^{-1} \sum F_i$ to be the average qubit fidelity of the full map $M = \bigotimes_i M_i$ over all components. The probability that the “noisy” qticket resulting from this map is accepted as valid is given by $p_{\text{h}}(M) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^\rho M(\rho)]$.

Theorem 6 (Soundness of qtickets) *As long as $F_{\text{exp}} > F_{\text{tol}}$, an honest holder can successfully redeem qtickets with a probability*

$$p_{\text{h}}(M) \geq 1 - e^{-ND(F_{\text{tol}} \| F_{\text{exp}})}.$$

Proof. Consider the boolean random variables $\vec{X} = (X_1, \dots, X_N)$ with joint distribution given by

$$\Pr[\vec{X} = \vec{b}] = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr} \left[M(\rho) \bigotimes_{i=1}^N (b_i \rho_i + \bar{b}_i \rho_i^\perp) \right]. \quad (\text{S2})$$

Since $M = \bigotimes_i M_i$, we may recast Eqn. S2 as

$$\Pr[\vec{X} = \vec{b}] = \prod_{i=1}^N \frac{1}{6} \sum_{\rho_i \in \tilde{Q}} \text{Tr} [M_i(\rho_i)(b_i \rho_i + \bar{b}_i \rho_i^\perp)] \quad (\text{S3})$$

Since \tilde{Q} is a quantum state 2-design over qubit space, each factor coincides with the definition of the average fidelity F_i of M_i if $b_i = 1$ and with $1 - F_i$ if $b_i = 0$. Hence the X_i are independent boolean random variables with probability $\Pr[X_i] = F_i$. Moreover, according to definition 5, we have $\frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[P_{\text{acc}}^\rho M(\rho)] = \Pr[\sum_{i=1}^N X_i \geq F_{\text{tol}}N]$. Since the X_i are independent, a standard Chernoff-Hoeffding bound allows us to conclude. ■

S.2.3. Security

The security statement expresses that for a sufficiently large security parameter $F_{\text{tol}} > 5/6$, the average probability of a dishonest participant successfully forging two accepted qtickets from a single one is exponentially small in N . Indeed, when simultaneously submitting two qtickets produced by applying the most general possible transformation T (a CPTP map) on a single valid qticket, the probability of both of them being accepted is exponentially small in N as long as we are not given access to the classical description.

Definition 7 (Counterfeiting fidelity) *We define the average counterfeiting fidelity of a map $T \in \mathcal{H}_Q \rightarrow \mathcal{H}_Q^{\otimes 2}$ as*

$$p_{\text{d}}(T) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr} \left[(P_{\text{acc}}^\rho)^{\otimes 2} T(\rho) \right] \quad (\text{S4})$$

The following is one of the main results and states that as long as the verification threshold F_{tol} is set sufficiently high a counterfeiter will have negligible chances of producing two valid qtickets from a single genuine original.

Theorem 8 (*Security of qtickets*) For $F_{\text{tol}} > 5/6$ and for any CPTP map $T \in \mathcal{H}_Q \rightarrow \mathcal{H}_Q^{\otimes 2}$ we have that

$$p_d(T) \leq e^{-ND(2F_{\text{tol}}-1\|2/3)}. \quad (\text{S5})$$

Most of the work for proving this goes into excluding the possibility that a non-product counterfeiting strategy could perform significantly better than any product strategy such as performing optimal cloning on each individual qubit. That is, we take into account the fact that the map T need not factorize with respect to the different components of the qticket. Note also that $D(2F_{\text{tol}} - 1\|2/3) = 0$ precisely for $F_{\text{tol}} = 5/6$ and is positive otherwise. Finally, we prove that even if the holder of a qticket attempts to perform v successive verification attempts (each time possibly using information learned from the acceptance/rejection of previous attempts) the chances of having two or more submitted qtickets accepted grows by no more than a factor of $\binom{v}{2}$.

Theorem 9 (*Security of qtickets with learning*) If the holder of a valid qticket submits v tokens for verification, the probability of having two or more accepted is upper bounded by

$$p_{d,v} = \binom{v}{2} e^{-ND(2F_{\text{tol}}-1\|2/3)}.$$

Note that since $\binom{v}{2}$ is a polynomial of degree 2 in v , this bound still allows for an exponentially large number (in N) of qticket submissions v , while preserving exponentially good security.

1. Proof outline

We now outline the proof for theorems 8 and 9. First, the claim in theorem 8 is equated to an equivalent one, which averages over the set of all pure product states instead of Q . We then bound the average cloning probability by $(2/3)^N$ for the set of pure product states following the lines of R. F. Werner [S4] for the optimal cloning of pure states. From there, the generalized Chernoff bound from theorem 3 for dependent random variables allows us to derive the desired result. The result of theorem 9 is obtained from a counting argument relating the security of multiple verification attempts with the static counterfeiting fidelity bound of theorem 8.

2. Equivalence with continuous statement

For the qticket protocol, drawing each component from a discrete set of states is required in order to provide an efficient classical description. However, certain statements are simpler to analyze over the full set of pure product states. This is the case for the counterfeiting fidelity, which can also be expressed as a uniform average over all pure product states.

Lemma 10 (*Counterfeiting fidelity*) The average counterfeiting fidelity of a map T can be expressed as

$$p_d(T) = \int d\vec{\rho} \quad \text{Tr} \left[(P_{\text{acc}}^{\vec{\rho}})^{\otimes 2} T(\vec{\rho}) \right] \quad (\text{S6})$$

where $\int d\vec{\rho}$ represents N nested integrations on the Haar measure of qubit components and $\vec{\rho}$ the resulting product state.

Proof. Definition 5 may seem unnecessarily cumbersome, yet it serves to make explicit that the projector P_{acc}^{ρ} is a polynomial of degree 1 in each of the components ρ_i of the qticket ρ . Furthermore, note that regardless of what the multi-qubit map T is, its application $T(\rho)$ has degree 1 in each of the components ρ_i of ρ . Together this implies that the integrand of lemma 10 is an polynomial of degree at most 3 in each of the qubit components ρ_i of $\vec{\rho}$. We may conclude by observing that the average taken in definition 7 is equivalent to uniformly taking each component ρ_i from a qubit state 3-design. ■

3. Optimal cloning for pure product states

R. F. Werner [S4] obtained a tight upper bound for the average probability of a CPTP map T producing m clones from n copies of an unknown pure quantum state $|\psi\rangle$. Our statement is that if one attempts to clone an N component pure product state, the optimal cloning probability is achieved by independently cloning each of the components; neither generating entanglement nor correlations may help with the cloning. We present this statement for the case of cloning two copies from a qubit product state, but the derivation is fully generalizable.

Lemma 11 (*Optimal cloning of pure product states*) The average cloning fidelity over N qubit component pure product states of a CPTP map T is bounded by

$$\int d\vec{\rho} \text{Tr}[\vec{\rho}^{\otimes 2} T(\vec{\rho})] \leq (2/3)^N.$$

Proof. One possible derivation of this lemma is by following the lines of the original proof for optimal cloning of pure states [S4]. First one shows that if there is a cloning map T achieving average fidelity F^* then there is a covariant cloning T^* achieving the same average fidelity. This map can be explicitly constructed as

$$T^*(\vec{\rho}) = \int d\vec{g} \quad \vec{g}^{\dagger \otimes 2} T(\vec{g}\vec{\rho}\vec{g}^{\dagger}) \vec{g}^{\otimes 2}, \quad (\text{S7})$$

where the integral $\int d\vec{g}$ averages over all possible local rotations \vec{g} on N subsystems. This covariant map achieves exactly the same cloning fidelity for any initial pure product state since all pure product states are equivalent up to local unitaries. Finally, we observe

$$0 \leq \text{Tr}[\vec{\rho}^{\otimes 2} T^*(\mathbb{1}_{2^N} - \vec{\rho})] \quad (\text{S8})$$

since $\mathbb{1}_{2^N} - \vec{\rho}$ is positive and T^* positivity preserving. We then obtain

$$F^* \leq \text{Tr}[\vec{\rho}^{\otimes 2} T^*(\mathbb{1}_{2^N})] \quad (\text{S9})$$

and may now average this inequality over $\vec{\rho}$ and use

$$\int d\vec{\rho} \quad \vec{\rho}^{\otimes 2} = \frac{(S_2)^{\otimes N}}{3^N}, \quad (\text{S10})$$

where S_2 is the rank 3 projector onto the symmetric space of two qubits. The operator norm of this expression is $1/3^N$ whereas $\text{Tr}[T^*(\mathbb{1}_{2^N})] \leq 2^N$ leading to $F^* \leq (\frac{2}{3})^N$, as desired. ■

4. Pigeonhole argument and Chernoff bound

We are now ready to prove the first no-counterfeiting result for qtickets.

Proof of theorem 8. Consider the boolean random variables $\vec{E} = (E_1, \dots, E_N)$ with joint distribution given by

$$\Pr[\vec{E} = \vec{b}] = \int d\vec{\rho} \text{Tr} \left[T(\vec{\rho}) \bigotimes_{i=1}^N (b_i \rho_i^{\otimes 2} + \bar{b}_i (\mathbb{1}_4 - \rho_i^{\otimes 2})) \right]. \quad (\text{S11})$$

Intuitively, the variable E_i represents the event of measuring the i -th component to be correctly cloned.

In order for the two qtickets to be accepted, there must be a total of at least $F_{\text{tol}}N$ components yielding the correct measured outcome in each qticket. By the pigeonhole principle, this means that there are at least $2F_{\text{tol}}N - N$ components which were measured correctly on both submitted qtickets,

$$p_d(T) \leq \Pr \left[\sum_{i=1}^N E_i \geq (2F_{\text{tol}} - 1)N \right]. \quad (\text{S12})$$

For arbitrarily chosen T , the E_i may be dependent variables. However, according to lemma 11, for any subset S of qubit components, we may bound

$$\Pr[\forall_{i \in S} E_i] \leq \left(\frac{2}{3} \right)^{|S|}. \quad (\text{S13})$$

Theorem 3, is now invoked to provide an upper bound on the RHS of eq. 12, yielding the thesis of theorem 8. ■

5. Combinatorial bound on learning

The bound on counterfeiting that we have provided assumes that two (possibly entangled) counterfeits are produced by applying a CP map on a single original copy. In contrast, a sequential strategy temporally orders the submitted qtickets where the production strategy (CP map) for the later submissions can depend on whether previous submissions were accepted or not. The counterfeiter may learn valuable information about how to construct valid qtickets from the feedback provided by the verifiers. The content of theorem 9 is that even with a valid qticket and the information learned from v repeated submissions it is very unlikely for a counterfeiter to produce more than one accepted qticket.

Proof of theorem 9. According to theorem 8, the probability $p_d(T)$ for any CP map T to produce two valid counterfeit copies from a single one, is upper bounded by $B = e^{-ND(2F_{\text{tol}}-1||2/3)}$. We bound the counterfeiting probability of an interactive strategy S submitting v tokens for verification by the sum of the counterfeiting fidelity of $\binom{v}{2}$ CP maps

$T_{k,l}$. Each of these maps corresponds to the case in which a specific pair (k, l) of the v submitted tokens are the first to be accepted by the verifiers.

Without loss of generality, we assume that in an interactive strategy the holder waits for the outcome of the j -th verification in order to decide how to continue and produce the $j+1$ -th submission. We model a v step interactive strategy S as a collection of CPTP maps $\{S_{\vec{b}}\}$ with \vec{b} a boolean string of length between 0 and $v - 1$ representing what the counterfeiter does after receiving the first $\text{len}(\vec{b})$ verification outcomes.

Each $S_{\vec{b}}$ is a CPTP map from \mathcal{H}_H to $\mathcal{H}_Q \otimes \mathcal{H}_H$, where \mathcal{H}_Q is a Hilbert space accommodating qtickets and \mathcal{H}_H is a larger space representing the memory of the holder.

For any partial verification result \vec{b} we may write the CPTP map which produces the $\text{len}(\vec{b})$ submissions as $\tilde{S}_{\text{tl}(\vec{b})}$, which is composed of successively applying $S_{\vec{b}'}$ for all initial substrings \vec{b}' of \vec{b} . That is

$$\begin{aligned} \tilde{S}_{\emptyset} &:= S_{\emptyset} \\ \tilde{S}_{\vec{b}} &:= (\text{id}_Q^{\otimes \text{len}(\vec{b})} \otimes S_{\vec{b}}) \circ \tilde{S}_{\text{tl}(\vec{b})}. \end{aligned} \quad (\text{S14})$$

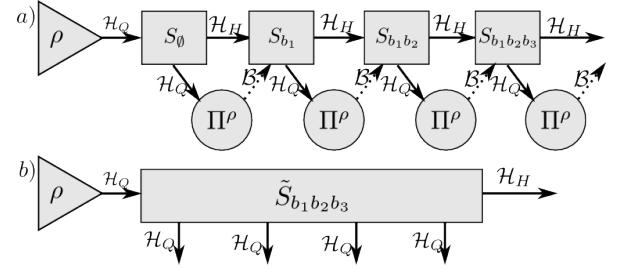


Figure S1: a) We schematically illustrate how a dynamical strategy S works. Each step of a strategy (grey rectangles) is a CPTP map $S_{\vec{b}}$ which depends on the classical outcome \vec{b} of previous verifications. The first map S_{\emptyset} takes an original qticket ρ as input, whereas subsequent steps rely on an internal memory state of the holder. The content of internal memory could range from no information at all, to a full original qticket and a detailed register of previous submissions. The verifiers have a fixed strategy Π^{ρ} which consists of applying the measurement $\{P_{\text{acc}}^{\rho}, P_{\text{rej}}^{\rho}\}$ and only returning the classical boolean measurement outcome. b) By fixing the classical input \vec{b} to the strategy, a CPTP map $\tilde{S}_{\vec{b}} \in \mathcal{H}_Q \rightarrow \mathcal{H}_Q^{\otimes \text{len}(\vec{b})+1} \otimes \mathcal{H}_H$ is constructed, corresponding to one possible partial application of the strategy S . This CPTP map produces $\text{len}(\vec{b}) + 1$ possibly entangled outputs in \mathcal{H}_Q from a single input qticket.

For an interactive strategy S the probability that the first $\text{len}(\vec{b})$ verification outcomes are given by \vec{b} is expressed as

$$p_{\vec{b}}(S) = \frac{1}{|Q|} \sum_{\rho \in Q} \text{Tr}[\tilde{S}_{\text{tl}(\vec{b})}(\rho)] \bigotimes_{j=1}^{\text{len}(\vec{b})} \left(b_j P_{\text{acc}}^{\rho} + \bar{b}_j P_{\text{rej}}^{\rho} \right) \otimes \mathbb{1}_H, \quad (\text{S15})$$

where $P_{\text{rej}}^{\rho} := \mathbb{1}_Q - P_{\text{acc}}^{\rho}$. The probability for the interactive strategy S to succeed at counterfeiting in v steps can be described as the sum of these probabilities over all possible full

verification outcomes including at least two acceptances

$$p_{d,v}(S) = \sum_{\substack{\vec{b}: \sum b_i \geq 2 \\ \text{len}(\vec{b})=v}} p_{\vec{b}}(S). \quad (\text{S16})$$

The key idea now is to use $p_{\vec{b}}(S) = p_{\vec{b}0}(S) + p_{\vec{b}1}(S)$ to provide an alternate expression for this sum. Namely, we combine verification outcomes starting in the same way into a single summand while avoiding the inclusion of failed counterfeiting attempts. Each full verification outcome containing two or more successful verifications has a unique shortest initial substring containing exactly two successful verifications. That a given substring is the shortest can be guaranteed by taking the last verification of the substring to be one of the two accepted.

$$p_{d,v}(S) = \sum_{\substack{\vec{b}: \sum b_i = 2 \\ b_{\text{len}(\vec{b})}=1}} p_{\vec{b}}(S). \quad (\text{S17})$$

Each of the $\binom{v}{2}$ summands on the RHS of Eq. (S17), may be characterized by two indices k, l s.t.

$$\vec{b} = \overbrace{0 \dots 0}^{k-1} 1 \overbrace{0 \dots 0}^{l-k-1} 1 \quad \text{for some } k < l \leq v. \quad (\text{S18})$$

For each one of these summands, we construct a static strategy $T_{k,l}(\rho) = \text{Tr}_{\setminus k,l}[\tilde{S}_{\text{tl}}(\vec{b})(\rho)]$ which takes as input a single valid qticket ρ and submits exactly two tokens. The counterfeiting probability of this map on ρ is

$$\begin{aligned} & \text{Tr} \left[(P_{\text{acc}}^{\rho})^{\otimes 2} T_{k,l}(\rho) \right] \\ &= \text{Tr} \left[(P_{\text{acc}}^{\rho})^{\otimes 2} \text{Tr}_{\setminus k,l} [\tilde{S}_{\text{tl}}(\vec{b})(\rho)] \right] \\ &= \text{Tr} [\tilde{S}_{\text{tl}}(\vec{b})(\rho) \bigotimes_{j=1}^{\text{len}(\vec{b})} (b_j P_{\text{acc}}^{\rho} + \bar{b}_j \mathbb{1}_Q) \otimes \mathbb{1}_H] \\ &\geq \text{Tr} [\tilde{S}_{\text{tl}}(\vec{b})(\rho) \bigotimes_{j=1}^{\text{len}(\vec{b})} (b_j P_{\text{acc}}^{\rho} + \bar{b}_j P_{\text{rej}}^{\rho}) \otimes \mathbb{1}_H]. \end{aligned} \quad (\text{S19})$$

By averaging over $\rho \in Q$ we obtain $p_{\vec{b}}(S) \leq p_d(T_{k,l}) \leq B$ and invoking Eq. (S17) we obtain $p_{d,v}(S) \leq \binom{v}{2} B$. ■

S.2.4. Tightness

For $F_{\text{tol}} < 5/6$ applying an optimal qubit cloning map[S4] $\Lambda(\rho) = \frac{1}{3}\rho \otimes \rho + \frac{1}{6}\rho \otimes \mathbb{1} + \frac{1}{6}\mathbb{1} \otimes \rho$ on each of the individual qubits of the qticket provides a good counterfeiting probability. The plot in Fig. S2 illustrates the probability of counterfeiter to actually get two qtickets accepted when taking this approach. For each of the two counterfeited qtickets, the probability of failing verification is the cumulant of a binomial distribution $B(N, 5/6)$ up to $F_{\text{tol}}N$ and rejection probability may be upper bounded by $\frac{1}{2} \exp(-2N(5/6 - F_{\text{tol}})^2)$ using

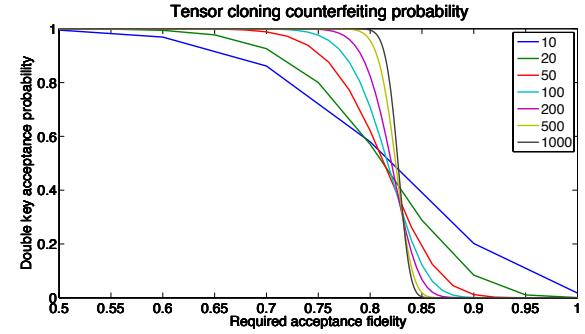


Figure S2: We numerically calculate the probability of accepting two copies of a qticket when the adversary strategy is assumed to be independently cloning each of the N qubits using an optimal cloning map. We see that the probability of producing two accepted qtickets approaches a step function at $5/6$ with N .

Hoeffding's inequality. Even when failure of the two qtickets is anticorrelated, the probability of either of them failing verification can not exceed the sum. This shows that the scheme can not be made secure for $F_{\text{tol}} < 5/6$. While such a scheme provides optimal forging probability when ($F_{\text{tol}} = 1$), other schemes could in principle outperform it in terms of counterfeiting capability. Although this is in principle possible, our security result shows that asymptotically in N , no other strategy may work for $F_{\text{tol}} > 5/6$.

S.2.5. Extension: Issuing multiple identical qtickets

Our results admit generalization to a scenario where the c identical copies of each qtickets are issued and successful verification of $c+1$ is to be excluded. To obtain an analog of lemma 10 requires the individual qubits composing a qticket to be drawn at random from a state t -design with $t = c+(c+1)$ (for example $t = 5$ would already be needed if two identical copies are issued). The optimal $c \rightarrow c+1$ cloning probability for N component product states is in this case bounded by $\left(\frac{c+1}{c+2}\right)^N$. The threshold fidelity required to guarantee security is then given by $F_{\text{tol}} > 1 - \frac{1}{(c+1)(c+2)}$. For such an F_{tol} , the analogous result to theorem 8 one obtained is

$$p_{c \rightarrow c+1}(T) \leq e^{-ND\left((c+1)F_{\text{tol}} - c\right)\left(\frac{c+1}{c+2}\right)}. \quad (\text{S20})$$

Finally, if $v > c+1$ verification attempts are allowed, the probability of counterfeiting can be proven not to grow faster than $\binom{v}{c+1}$. The proofs of these claims completely follow the lines that have been presented. Striving for legibility, we have limited the proof presented to $c = 1$, thus avoiding the notational burden imposed by the extra indices required.

S.3. CV-QTICKETS

In this section we provide a proof that cv-qtickets are secure, not only against counterfeiting but also against any other possible double usage. We first present definitions for cv-qtickets and their verification. We then state the associated soundness and security guarantees and outline the security proof. Only the proof of the security statement is provided, since proving soundness for cv-qtickets requires no additional techniques as compared to soundness of qtickets.

S.3.1. Definition of cv-qticket

Each cv-qticket is composed of $n \times r$ qubit pairs. Each qubit pair is prepared by choosing a state from

$$\{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |-,0\rangle, |+,1\rangle, |-,1\rangle\}$$

uniformly at random.

A full verification question for the cv-qticket will consist of n randomly chosen axes from $\{X, Z\}$ each corresponding to a specific block of r qubit pairs. In principle, the holder of the cv-qticket then measures the polarization of every qubit components along the corresponding requested axis and communicates the measurement outcomes to the verifier. The criteria to consider an answer correct is the following; within each of the n blocks, at least $F_{\text{tol}}r$ of the reported outcomes corresponding to qubits prepared in a polarization eigenstate of the inquired axis should be given correctly.

S.3.2. Soundness

The soundness result states that even under imperfect storage and readout fidelity, legitimate cv-qtickets work well as long as the fidelity loss is not too severe. Again, the completely positive trace preserving (CPTP) maps M_j will be assumed to represent the encoding, storage and readout of the j -th qubit component of the cv-qticket, with the full map over all components given by $M = \bigotimes_{j \in \{1, \dots, 2r \times n\}} M_j$. In the case of cv-qtickets, sufficiently many ($F_{\text{tol}}r$) correct answers should be provided within each block, demanding that a sufficiently good average fidelity be implemented for every single block. A random remapping of the Cartesian axes for each qubit component of a cv-qticket is also necessary, and can be achieved via a random unitary (possibly from a unitary 2-design). This is required for example in the case where an actual physical polarization, say X , is lost faster than other components. In this case asking for the stored X polarization for all qubits in a block may yield a large failure probability even though the average storage fidelity among the qubits is sufficiently high. A random unitary remapping solves this and allows to connect with the average qubit storage fidelity, even in the case where only two nominal axes are used.

Given $F_j = F(M_j)$, the average fidelity of the qubit map M_j , we define $F_{\text{exp},b} := N^{-1} \sum_{j: \lceil \frac{j}{2r} \rceil = b} F_j$ to be the average qubit fidelity within block $b \in \{1, \dots, n\}$. Further-

more, to simplify the final expression, let us define $F_{\text{exp}} = \min_b F_{\text{exp},b}$.

Theorem 12 (*Soundness of cv-qtickets*) *As long as $F_{\text{exp}} > F_{\text{tol}}$, an honest holder implementing a map M can successfully redeems cv-qtickets with a probability*

$$p_{\text{h}}^{\text{cv}}(M) \geq \left(1 - e^{-rD(F_{\text{exp}} \| F_{\text{tol}})}\right)^n.$$

Observe that one may reduce this statement to n independent statements within each block which are completely analogous to the soundness for qtickets theorem 6.

S.3.3. Security

A naive security statement expresses that the holder of a single cv-qticket is unable to produce two copies from it, each with the potential of passing a verification. Since the verification of cv-qtickets is achieved by sending a classical message to a verifier, the security statement for cv-qtickets goes beyond this; it states that even with simultaneous access to two randomly chosen verification questions, the holder of a cv-qticket is exponentially unlikely to provide satisfactory answers to both. We further extend our security claim, to an even more adverse scenario; the holder of a cv-qticket has simultaneous access to v independent verification questions and may proceed to answer them in any chosen order. Moreover failing in verification attempts does not forbid the holder from further attempts which may possibly be performed relying on the information accumulated from previous verification outcomes.

Let S be a mathematical object denoting the counterfeiting strategy taken by the holder of a valid cv-qticket. We will denote by $p_{\text{d},v}^{\text{cv}}(S)$, the probability that strategy S leads to two or more successful verifications when engaging in v verification attempts with possibly independent verifiers. The probability is taken over the random generation of cv-qtickets, of verification questions, and of measurement outcomes (Born's rule). The security statement is then

Theorem 13 (*Security of cv-qtickets*) *For any counterfeiting strategy S and tolerance parameter $F_{\text{tol}} > \frac{1+1/\sqrt{2}}{2}$ we have*

$$p_{\text{d},v}^{\text{cv}}(S) \leq \binom{v}{2}^2 \left(1/2 + e^{-rD(F_{\text{tol}} \| \frac{1+1/\sqrt{2}}{2})}\right)^n.$$

The proof of this statement goes as follows. Since abstractly cv-qtickets consist of a set of randomly produced states and questions requested on these states the formalism of quantum retrieval games (QRGs) provides adequate modeling. This framework is presented in a largely self-contained manner, since its generality and potential make it of independent interest. We first provide basic definitions for QRGs and derive some simple results. Then we present possible ways of composing QRGs together with associated quantitative bounds. The first results are then applied to the qubit pair constituents of cv-qtickets to bound the holders potential to provide answers to complementary question. Cv-qtickets are

then modeled by a QRG for scenarios in which the holder of a cv-qticket wishes to simultaneously answer questions from two independent verifiers without any additional aid. Finally, a combinatorial bound, similar to the one used for qtickets, is used to provide an upper limit on how the double verification probability may increase with the number v of verification attempts.

S.3.4. Quantum retrieval games

Quantum retrieval games (QRGs), recently defined by Gavinsky [S5] provide a framework to analyze protocols in which information is to be extracted from a state produced according to a classical probability distribution. We will here present a definition of QRGs following Gavinsky as well as some additional results derived which may be of independent interest.

Alice prepares a normalized state $\rho_s = \varrho(s)/p_s$ according to the probability $p_s := \text{Tr}[\varrho_s]$ and transfers it to Bob. Whereas Alice remembers the index s of the generated state, Bob is only provided with ρ_s and a full description of the distribution from which it was generated. Alice then asks Bob a question about s which Bob attempts to answer as best as possible. A simple possibility is for Alice to directly ask Bob the value of s . In general however, the set of possible answers A need not coincide with the set of indexes S over the possible prepared states. If each answer a is either correct or incorrect the question may be modeled as $\sigma \in S \times A \rightarrow \{0, 1\}$. This is, $\sigma(s, a) = 1$ iff the answer a is correct for state index s and $\sigma(s, a) = 0$ otherwise. This definition faithfully represents Gavinsky's QRGs. We extend this notion to weighted quantum retrieval games (WQRGs) to model situations where some answers are “more correct” than others. Here for each prepared state s and possible answer a the game will assign a non-negative real value $\sigma(s, a)$ associated to the utility function of answer a given input s (i.e. $\sigma \in S \times A \rightarrow \mathbb{R}_+$).

Bob needs to choose an answer $a \in A$ and may use his copy of state ρ_s to do so. The most general strategy that Bob can take according to the laws of quantum mechanics is to perform a positive operator valued measurement (POVM). We will consider post-selected POVMs, as opposed to a physical POVM, as those which may fail to produce a measurement outcome. This is, whereas a physical POVM always produces an outcome from the expected set, for post-selected POVM some “invalid” outcomes are discarded and excluded from statistics.

In order to express the random preparation of states by Alice we first define the notion of an indexed ensemble.

Definition 14 (Indexed ensemble) *We will say that ϱ is an ensemble on \mathcal{H} indexed over S iff $\forall s \in S : \varrho(s)$ is a positive operator on \mathcal{H} and $\sum_{s \in S} \text{Tr}[\varrho(s)] = 1$.*

Note that if ϱ is an indexed ensemble, then $\rho = \sum_s \varrho(s)$ is a normalized density matrix. Although Alice gives a specific state $\varrho(s)/\text{Tr}[\varrho(s)]$ to Bob, since Bob does not know s , he does not know which one has been received. The state $\rho = \text{Tr}_{Alice}[\sum_{s \in S} s \otimes \varrho(s)]$ will be called the reduced density

matrix of ϱ since it corresponds to tracing out Alice's classically correlated subsystem containing the index s . Without loss of generality, ρ can be assumed to be full rank on \mathcal{H} .

In other words, a physical/selective projection \mathcal{P} indexed over A is simply a physical/post-selected POVM equipped with an interpretation for each possible measurement outcome in terms of possible answers in $a \in A$.

Definition 15 (Selective and physical projections) *We will say that \mathcal{P} is a selective projection indexed over A iff $\forall a \in A$, $\mathcal{P}(a)$ are bounded positive semidefinite operators on \mathcal{H} . It will also be a physical projection iff $\sum_a \mathcal{P}(a) = \mathbb{1}$.*

Note that no normalization has been imposed for selective projections since induced probability distributions are normalized a posteriori. An indexed ensemble and a projection on the same Hilbert space induce a joint probability distribution over the indexes $S \times A$ of prepared states and provided answers.

Definition 16 (Induced probability distribution) *Let ϱ be an ensemble on \mathcal{H} indexed over S and let \mathcal{P} be a projection on \mathcal{H} indexed over A . Then*

$$p(s_0, a_0) = \frac{\text{Tr}[\mathcal{P}(a_0)\varrho(s_0)]}{\sum_{s,a} \text{Tr}[\mathcal{P}(a)\varrho(s)]}. \quad (\text{S21})$$

is a probability distribution over $S \times A$ which will be denoted by $p = \langle \varrho, \mathcal{P} \rangle$ and is undefined unless $\sum_{s,a} \text{Tr}[\mathcal{P}(a)\varrho(s)] > 0$.

Furthermore, note that for physical projections the denominator in Eq. (S21) is 1 and the marginal of the resulting distribution over S is $p(s) = \sum_a p(s, a) = \text{Tr}[\varrho(s)]$ which is independent of \mathcal{P} .

Definition 17 (Weighted quantum retrieval games) *Let ϱ be an ensemble on \mathcal{H} indexed over S . Consider a utility function $\sigma \in S \times A \rightarrow \mathbb{R}_+$. Then the pair $\mathcal{G} = (\varrho, \sigma)$ is a weighted quantum retrieval game. A WQRG is also a QRG when $\sigma \in S \times A \rightarrow \{0, 1\}$.*

The value of a game \mathcal{G} w.r.t. a projection \mathcal{P} is the average utility obtained by Bob by using a certain measurement strategy \mathcal{P} . This value is given by the expectancy of the utility function σ over the joint distribution of prepared states and measurement outcomes.

Definition 18 *The value of game $\mathcal{G} = (\varrho, \sigma)$ w.r.t. projection \mathcal{P} is defined as*

$$\text{Val}(\mathcal{G}, \mathcal{P}) := \sum_{s,a} p(s, a) \sigma(s, a) \quad (\text{S22})$$

where $p = \langle \varrho, \mathcal{P} \rangle$ is the induced probability distribution.

We now define the optimum value achievable by Bob for two distinct conditions depending on whether selective or physical projections are allowed.

Definition 19 *The selective (respectively physical) value of a game \mathcal{G} are defined as*

$$\text{Sel}(\mathcal{G}) := \sup_{\mathcal{P} \in \text{Selective projections}} \text{Val}(\mathcal{G}, \mathcal{P}) \quad (\text{S23})$$

$$\text{Phys}(\mathcal{G}) := \sup_{\mathcal{P} \in \text{Physical projections}} \text{Val}(\mathcal{G}, \mathcal{P}). \quad (\text{S24})$$

Note that according to this definition $\text{Sel}(\mathcal{G}) \geq \text{Phys}(\mathcal{G})$ since the supremum is taken over a larger set. However, for certain tailored games, the selective and physical values will coincide. The advantage of selective values is that they may be straightforwardly computed and are more amenable to compositional results. If Bob is forced to provide an answer, he can only achieve the physical value of a game. If Bob is allowed to abort the game after measuring his state ρ_s and aborted games are not considered when calculating his expected utility then he will be able to achieve the selective value.

The following result provides an explicit formula to calculate the selective value of a game. In this sense, it is a generalization of lemma 4.3 in [S5].

Theorem 20 (Selective value of a game) *Let $\mathcal{G} = (\varrho, \sigma)$ be a WQRG with $\sum_s \varrho(s) = \rho$. Define $O(a) := \sum_s \sigma(s, a) \rho^{-1/2} \varrho(s) \rho^{-1/2}$. Then the selective value of \mathcal{G} may be calculated as $\text{Sel}(\mathcal{G}) = \max_a \|O(a)\|$, where $\|\cdot\|$ denotes the operator norm.*

Proof. We first use the definition of the value of a game \mathcal{G} w.r.t. \mathcal{P} , expand the induced probability distribution and move the sum over s inside the trace

$$\text{Val}(\mathcal{G}, \mathcal{P}) = \frac{\sum_a \text{Tr}[\mathcal{P}(a) \sum_s \sigma(s, a) \varrho(s)]}{\sum_a \text{Tr}[\mathcal{P}(a) \sum_s \varrho(s)]}. \quad (\text{S25})$$

We define $\tilde{\mathcal{P}}$ such that $\tilde{\mathcal{P}}(a) = \rho^{1/2} \mathcal{P}(a) \rho^{1/2}$. Using this definition and that of ρ and O_a we may rewrite

$$\begin{aligned} \text{Val}(\mathcal{G}, \mathcal{P}) &= \frac{\sum_a \text{Tr}[\tilde{\mathcal{P}}(a) O(a)]}{\sum_a \text{Tr}[\tilde{\mathcal{P}}(a)]} \\ &\leq \max_a \frac{\text{Tr}[\tilde{\mathcal{P}}(a) O(a)]}{\text{Tr}[\tilde{\mathcal{P}}(a)]} \\ &\leq \max_a \|O(a)\|. \end{aligned} \quad (\text{S26})$$

The first inequality uses the positivity of all summands. For the second inequality we note that $\tilde{\mathcal{P}}(a)$ must be positive semidefinite and the variational definition of operator norm of the positive semidefinite operator $O(a)$. Equality can be achieved by taking $\tilde{\mathcal{P}}(a_0)$ to be a projector onto the highest eigenvalue subspace of $O(a_0)$ if $\|O(a_0)\| = \max_a \|O(a)\|$ and taking $\tilde{\mathcal{P}}(a_0) = 0$ otherwise. ■

The theorem provides an explicit construction of a projection achieving the selective value of a game. Furthermore, the proof allows us to derive a necessary and sufficient condition under which the selective and physical values of a game coincide.

Corollary 21 *Given a retrieval game \mathcal{G} , we have that $\text{Sel}(\mathcal{G}) = \text{Phys}(\mathcal{G})$ iff there exist positive $\tilde{\mathcal{P}}(a)$ such that*

$$O(a) \tilde{\mathcal{P}}(a) = \text{Sel}(\mathcal{G}) \tilde{\mathcal{P}}(a) \quad \text{and} \quad \sum_a \tilde{\mathcal{P}}(a) = \rho \quad (\text{S27})$$

We now turn to the systematic composition of retrieval games in the form of product and threshold games. This provides a way to construct more elaborate retrieval games together with bounds on their associated values. A natural definition of tensor product may be given for indexed ensembles, projections and utility functions.

$$(\varrho_1 \otimes \varrho_2)(s_1, s_2) = \varrho_1(s_1) \otimes \varrho_2(s_2) \quad (\text{S28})$$

$$(\mathcal{P}_1 \otimes \mathcal{P}_2)(a_1, a_2) = \mathcal{P}_1(a_1) \otimes \mathcal{P}_2(a_2) \quad (\text{S29})$$

$$(\sigma_1 \otimes \sigma_2)((s_1, s_2), (a_1, a_2)) = \sigma_1(s_1, a_1) \sigma_2(s_2, a_2) \quad (\text{S30})$$

These definitions have the property that the tensor product of physical projections is a physical projection and that the induced probability distribution of two tensor product is the tensor product of the individual induced probability distributions

$$\langle (\varrho_1 \otimes \varrho_2), (\mathcal{P}_1 \otimes \mathcal{P}_2) \rangle = \langle \varrho_1, \mathcal{P}_1 \rangle \otimes \langle \varrho_2, \mathcal{P}_2 \rangle$$

Definition 22 (Tensor product WQRG) *Let $\mathcal{G}_1 = (\varrho_1, \sigma_1)$ and $\mathcal{G}_2 = (\varrho_2, \sigma_2)$. We define the tensor product WQRG $\mathcal{G}_1 \otimes \mathcal{G}_2$ as*

$$\mathcal{G}_1 \otimes \mathcal{G}_2 = (\varrho_1 \otimes \varrho_2, \sigma_1 \otimes \sigma_2).$$

Proposition 23 (Tensor product selective value) *The selective value of a tensor product game is the product of the selective value of the independent games.*

$$\text{Sel}(\mathcal{G}_1 \otimes \mathcal{G}_2) = \text{Sel}(\mathcal{G}_1) \text{Sel}(\mathcal{G}_2)$$

Proof. By using the definition of $O(a)$ in theorem 20 with respect to the WQRG involved we obtain

$$\|O(a_1, a_2)\| = \|O_1(a_1) \otimes O_2(a_2)\| = \|O_1(a_1)\| \|O_2(a_2)\|.$$

Maximizing over a_1 and a_2 on both sides theorem 20 provides the desired equality. ■

The selective value of the product game is attained by the tensor product of projections, each achieving the respective selective values.

Corollary 24 (Tensor product physical value) *If $\text{Phys}(\mathcal{G}_1) = \text{Sel}(\mathcal{G}_1)$ and $\text{Phys}(\mathcal{G}_2) = \text{Sel}(\mathcal{G}_2)$ then $\text{Phys}(\mathcal{G}_1 \otimes \mathcal{G}_2) = \text{Sel}(\mathcal{G}_1 \otimes \mathcal{G}_2)$.*

Given a direct product game and a projection for it one may consider the inverse procedure of defining a projection on one of the subcomponents of the game.

Definition 25 (Restriction of a projection) *Let \mathcal{P} be a projection on $\mathcal{H}_1 \otimes \mathcal{H}_2$ indexed over $A_1 \times A_2$. Furthermore, let ρ_2 be a normalized density matrix on \mathcal{H}_2 . We define the restriction $\mathcal{P}_{|1}$ with respect to ρ_2 and A_2 as*

$$\mathcal{P}_{|1}(a_1) = \sum_{a_2} \text{Tr}_2(\mathcal{P}(a_1, a_2) \mathbb{1} \otimes \rho_2).$$

By abuse of notation, if $\rho = \rho_1 \otimes \rho_2$ is a normalized product state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ we may define the restriction of \mathcal{P} with respect to the normalized tensor factors of ρ . This is the case for the reduced density matrix of product indexed ensembles. By restricting a projection one obtains a new projection which induces the same reduced probability distribution

Lemma 26 (Restriction of a projection) Let $\mathcal{P}_{|1}$ be the restriction of \mathcal{P} with respect to ρ_2 and A_2 , where ρ_2 is the reduced density matrix of ϱ_2 . Then

$$\langle \varrho_1, \mathcal{P}_{|1} \rangle(s_1, a_1) = \sum_{s_2, a_2} \langle \varrho_1 \otimes \varrho_2, \mathcal{P} \rangle(s_1 s_2, a_1 a_2).$$

Theorem 27 (Selective value of threshold QRG) Let $\mathcal{G}_j = (\varrho_j, \sigma_j)$ be WQRGs s.t. $\sigma_j \in (S_j, A_j) \rightarrow [0, 1]$ and $\text{Sel}(\mathcal{G}_j) = \delta_j$ for all $j \in \{1, \dots, n\}$. Furthermore take $\delta = n^{-1} \sum_{j=1}^n \delta_j$ and $\delta \leq \gamma \leq 1$. Define the QRG $\mathcal{G}_\gamma = (\bigotimes_j \varrho_j, \sigma_\gamma)$ with a tensor product ensemble distribution and boolean utility function

$$\sigma_\gamma(\vec{s}, \vec{a}) = \left(\sum_{j=1}^n \sigma_j(s_j, a_j) \geq \gamma n \right).$$

Then we have $\text{Sel}(\mathcal{G}_\gamma) \leq 2e^{-nD(\gamma\|\delta)}$.

Proof. The direct product indexed ensemble $\varrho = \bigotimes_j \varrho_j$ and projection \mathcal{P} induce a normalized probability distribution over $\vec{S} \times \vec{A}$ given by

$$p(\vec{s}, \vec{a}) = \frac{\text{Tr}[\mathcal{P}(\vec{a})\varrho(\vec{s})]}{\sum_{\vec{s}\vec{a}} \text{Tr}[\mathcal{P}(\vec{a})\varrho(\vec{s})]}.$$

Define the dependent random variable X_j to be $\sigma_j(s_j, a_j)$ where s_j and a_j are taken according to this probability distribution. For any $S \subseteq \{1, \dots, n\}$, we may define $\mathcal{P}_{|S}$ as the restriction of the projection \mathcal{P} to the subsystems specified by S with respect to $(\varrho_{\vec{s}})$. By proposition 23 we have that

$$\text{Exp} \left[\prod_{j \in S} X_j \right] = \text{Val} \left(\bigotimes_{j \in S} \mathcal{G}_j, \mathcal{P}_{|S} \right) \leq \prod_{j \in S} \delta_j. \quad (\text{S31})$$

Using theorem 3 and definition 18 we obtain

$$\text{Val}(\mathcal{G}_\gamma, \mathcal{P}) = \mathbf{Pr} \left[\sum_j X_j \geq \gamma n \right] \leq 2e^{-nD(\gamma\|\delta)}. \quad (\text{S32})$$

Since this is true for arbitrary \mathcal{P} we conclude that $\text{Sel}(\mathcal{G}_\gamma) \leq 2e^{-nD(\gamma\|\delta)}$. ■

S.3.5. cv-ticket qubit pair building block

Consider a game in which Alice transfers to Bob one of the following states chosen at random

$$S = \{|0,+\rangle, |0,-\rangle, |1,+\rangle, |1,-\rangle, |+,0\rangle, |-,0\rangle, |+,1\rangle, |-,1\rangle\},$$

each with probability 1/8. Alice then asks Bob for the Z polarization of both qubits, possible answers being $A = \{00, 01, 10, 11\}$. An answer is correct iff it coincides in the polarization of the qubit prepared in a Z eigenstate. Bob can always answer the question correctly by measuring both qubits in the Z basis.

The quantum retrieval game formalism applies to this problem although one must admit that it is like cracking a nut with a sledgehammer. We call this game $\mathcal{G}_Z = (\varrho, \sigma_Z)$ where we have $\sum_s \varrho(s) = \rho = \mathbb{1}_4/4$, and $\text{Tr}(\varrho(s)) = 1/8$ for all $s \in S$. A formal definition of the utility function σ_Z can be given as $\sigma_Z(s, a) = (s_1 \equiv a_1 \text{ or } s_2 \equiv a_2)$. We first define the operators $O(a)$ from theorem 20. Due to symmetry we may restrict to considering one such operator

$$O(00) = 4(\varrho(0,+) + \varrho(0,-) + \varrho(+,0) + \varrho(-,0)) \quad (\text{S33})$$

and find that $\|O(00)\| = 1$ which is a non degenerate eigenvalue for all $O(a)$. The fact that the four corresponding eigenspaces are orthogonal confirms that 1 is also the physical value of the game.

The same trivial value of 1 can be achieved for the game in which Alice requests the X direction polarization of the states. We will call this game $\mathcal{G}_X = (\varrho, \sigma_X)$. The problem becomes interesting if Bob is requested provide a guess for both complementary polarizations. There are two relevant possibilities, both of which will require Bob to give an answer twice as long as before. The first scenario describes the best case probability of Bob answering both questions correctly and may be modeled by a QRG with utility function

$$\mathcal{G}_\wedge = (\varrho, \sigma_\wedge) \quad \sigma_\wedge(s, a_X a_Z) = \sigma_X(s, a_X) \wedge \sigma_Z(s, a_Z).$$

In the second scenario we are interested in the average number of questions answered correctly when two complementary questions are posed and may be modeled by the WQRG with utility function

$$\mathcal{G}_{\text{avg}} = (\varrho, \sigma_{\text{avg}}) \quad \sigma_{\text{avg}}(s, a_X a_Z) = \frac{\sigma_X(s, a_X) + \sigma_Z(s, a_Z)}{2}.$$

Thanks to symmetries one need only calculate a single $\|O(a)\|$ and for concreteness we choose $O(+-00)$. For the conjunction QRG we obtain

$$O(+-00) = 4(\varrho(0,+) + \varrho(+,0)) \text{ and } \|O_{+-00}\| = 3/4.$$

For the average WQRG we obtain

$$O(+-00) = 2[2\varrho(0,+) + 2\varrho(+,0) + \varrho(0,-) + \varrho(-,0) + \varrho(+,1) + \varrho(1,+)] \quad (\text{S34})$$

and $\|O_{+-00}\| = 1/2 + 1/\sqrt{8} \approx 0.8536$. This is precisely the optimal fidelity for covariant qubit cloning (i.e. cloning of equatorial qubits). On the other hand, if Bob is asked the same question twice instead of complementary questions it is clear that he will be able to repeat two correct answers. All in all, if Bob is asked complementary question half of the time and coinciding questions half of the time he will be able to emulate an average fidelity of $3/4 + \sqrt{2}/8 \approx 0.927$.

Indeed, once we have defined a concrete WQRG, calculating its selective value becomes an exercise thanks to theorem 20. Furthermore, if the game has sufficient symmetry it will be possible to prove a coinciding physical values for the game.

S.3.6. cv-qticket

We will first bound the probability of answering two of these randomly chosen questions by bounding the selective value of the corresponding retrieval game. To do this, we bound the value of a game where r complementary questions are asked on r qubit pairs (this is precisely the case for one block when the two random questions are complementary).

$$\begin{aligned}\sigma_{F_{\text{tol}}}^{(X)}(\vec{s}, \vec{a}^{(X)}) &= \left(\sum_{j=1}^r \sigma_j^{(X)}(s_j, a_j^{(X)}) \geq F_{\text{tol}}r \right) \\ \sigma_{F_{\text{tol}}}^{(Z)}(\vec{s}, \vec{a}^{(Z)}) &= \left(\sum_{j=1}^r \sigma_j^{(Z)}(s_j, a_j^{(Z)}) \geq F_{\text{tol}}r \right) \\ \sigma_{F_{\text{tol}}}^{\wedge}(\vec{s}, (\vec{a}^{(X)}, \vec{a}^{(Z)})) &= \sigma_{F_{\text{tol}}}^{(X)}(\vec{s}, \vec{a}^{(X)}) \wedge \sigma_{F_{\text{tol}}}^{(Z)}(\vec{s}, \vec{a}^{(Z)})\end{aligned}\quad (\text{S35})$$

We will not calculate the selective value exactly but give a bound in terms of theorem 27. In order for the two block answers to be correct, among the two, at least $2F_{\text{tol}}r$ answers should have been provided correctly for individual qubit pairs. This is a weaker condition since it only imposes that the sum among the two block answers be sufficiently large, not necessarily implying that they are both above threshold.

$$\sigma_{F_{\text{tol}}}^{\wedge}(\vec{s}, (\vec{a}^{(X)}, \vec{a}^{(Z)})) \leq \left(\sum_{j=1}^r \sigma_j^{\text{avg}}(s_j, (a_j^{(X)}, a_j^{(Z)})) \geq F_{\text{tol}}r \right) \quad (\text{S36})$$

The description on the right hand side has precisely the form required for theorem 27. We conclude that the selective value and hence the probability within any strategy of providing valid answers to two complementary questions for the same block is upper bounded by $2 \exp[-rD(F_{\text{tol}}||1/2 + 1/\sqrt{8})]$ (for $F_{\text{tol}} > 1/2 + 1/\sqrt{8}$).

Given two randomly chosen questions for a block there is a probability of $1/2$ that they will coincide and a probability $1/2$ that they will be complementary. Taking this into account, the probability for a dishonest holder to correctly answer two such randomly chosen block questions is upper bounded by $1/2 + \exp[-rD(F_{\text{tol}}||1/2 + 1/\sqrt{8})]$. By taking r sufficiently large, this value can be guaranteed to be smaller than 1 . Hence, the probability of correctly answering n such randomly chosen threshold question pairs will be upper bounded by $B := (1/2 + \exp[-rD(F_{\text{tol}}, 1/2 + 1/\sqrt{8})])^n$ which can be made exponentially close to 1 in n .

S.3.7. Combinatorial bound on choosing and learning

The formulation presented adequately models a scenario in which the holder of a cv-qticket does not receive any feedback from the verifiers. However, if the holder of a cv-qticket can engage in several verification protocols, new possibilities arise which should be taken into account.

Firstly, by simultaneously engaging in several (v) verification protocols with different verifiers, the holder may simultaneously have access to v challenge questions. The holder may then for instance, choose the most similar questions and attempt to answer these. Furthermore, by successively participating in v verification protocols the holder can choose to perform verifications sequentially and wait for the outcome of the k -th before choosing which question to answer as the $k+1$ -th and providing an answer for it.

In general, if the holder engages in v verification attempts, he will receive v random questions providing no additional information on the cv-qticket. There are $\binom{v}{2}$ possible question pairs among these, each of which can be seen as randomly chosen. Thus if no feedback is used the probability of answering at least one of these pairs correctly is upper bounded by $\binom{v}{2}B$. An example scenario where this bound is relatively tight is when r is very large and n is relatively small. In this case, the probability of answering two randomly chosen questions is well approximated by the collision probability 2^{-n} (i.e. the probability that two questions coincide) which grows precisely as $\binom{v}{2}$ if the holder has access to v independently drawn questions and may choose to answer any pair.

Suppose now, that the answers to the verifiers are provided sequentially, so that the decision of which answer to produce for each verifier may be made dependent on the outcome of previous verifications. We can safely assume that the answers to challenge questions are then provided sequentially, each after receiving the acceptance or rejection of the previous ones. We can then apply a similar argument to the one exposed for the proof of qticket security in section S.2 S.2.3.5. This yields an additional factor of $\binom{v}{2}$ corresponding to the possible feedback scenarios up to the point of the second accepted answer, each of which can be simulated statically (i.e. by assuming the given feedback and fixing a corresponding POVM to generate answer up to that point). Hence the total probability for an interactive strategy with v verification attempts of producing two or more accepted answers is upper bounded by $\binom{v}{2}^2B$.

It may seem artificial for verifiers to select a random question each time. Randomness is important in order to avoid revealing information about the issued cv-qticket. However, the verifier may choose a random question once and for all and ask it until it is answered correctly. Once it has been answered correctly, the verifier knows that the cv-qticket has already been redeemed and can thus reject all subsequent verification attempts. This is similar to the kind of scheme used for prepaid telephone cards discussed in the applications section. However, the quantum case provides an advantage since one may have multiple verifiers which do not communicate. In a simple example with two verifiers, two composite questions may be chosen such that they are complementary on every qubit pair (i.e. one question is chosen at random and uniquely determines the other).

S.4. APPLICATIONS

Our quantum information application attempts to reduce quantum requirements to a minimum. However, even prepare

and measure qubit memories remain technologically challenging. For problems admitting a classical solution, such an approach is likely to be technologically less demanding. In other words, relevant applications for prepare and measure quantum memories will be those solving problems for which no classical solutions are known. In this section we discuss some problems with classical solutions and propose refinement of such problems for which no classical solution is possible.

S.4.1. Enforcing single usage with a single verifier

For some applications, the no cloning of quantum information is only an apparent advantage. Our qticket and cv-qticket constructions can guarantee an exponentially small double usage probability. However, this is not an impressive feat for scenarios where there is a single verifier or if the verifiers have access to realtime communication with a centralized database. In this case, a randomly chosen classical ticket has equally good properties. After a ticket is successfully redeemed once, it can be removed from the central database, making it invalid for any successive verification attempt. In fact this classical strategy is widely used for crediting prepaid phone lines with a client calling a toll free number and typing the purchased ticket number in order to credit a telephone account. Thus in such scenarios, the quantum strategy does not provide additional protection with respect to a classical solution.

S.4.2. Multiple non communicating verifiers

In scenarios with multiple non communicating verifiers, (cv-)qtickets provide a solution to a problem where all classical approaches fail. We describe a *witness protection program* as an example of how such a scenario might look like.

In a witness protection program, a governmental institution decides to give asylum to a key eye witness to whom an unforgeable quantum token is issued. This token can be used by the witness (holder) to claim asylum in any of a set of participating hotels (verifiers). The issuer also provides all hotels with the necessary information to verify the tokens. When using the token, neither the eye-witness nor the chosen hotel wish to divulge the locale where the witness is hosted, thus protecting both from being targets of an attack. This includes suspending communication between participating hotels as well as with the issuing authority. Any classical solution can not prevent a sufficiently resourceful holder from making copies of the received token, thus hotels are forced to communicate in order to avoid its double use. In this case, a quantum solution based on unforgeable tokens is the sole possibility to satisfy these unique constraints.

S.4.3. Reduced availability under sporadic verification

In principle, a centralized database may guarantee that classical ticket are only redeemed once. However, there are situations where the ticket should be available only to one holder

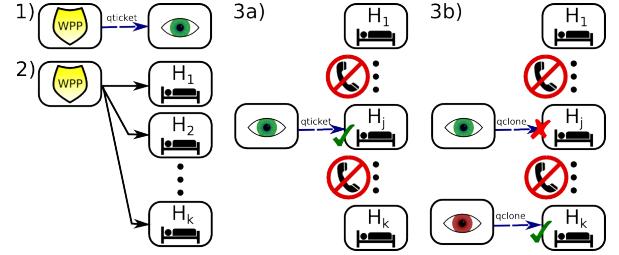


Figure S3: 1) The issuing entity hands a qticket to the key witness. 2) It provides the hotels with the secret classical description which will be used to verify it. 3a) An honest witness chooses a hotel and physically transfer the qticket for verification. It will be accepted as long as the level of accumulated noise is below threshold. 3b) A dishonest witness will fail to counterfeit his/her qticket to provide acommodation for an additional guest. However, there is no way of avoiding a valid qticket from changing hands.

at a time and the non-clonable nature of a qticket allows enforcing this. One such example is the sporadic control of tickets required for a given service. For concreteness, imagine a qticket which is valid for making use of a public transportation network. Commuters are sporadically controlled, at which point if they are found to have an invalid qticket they are charged an important fine, whereas if they are found to hold a valid qticket, they are provided with a fresh substitute. If the transportation tickets are classical, sporadic control can not avoid counterfeited copies in the hands of coluding commuters from circulating simultaneously. The deceiving commuters need only communicate classically among each other before and after they are controlled, effectively sharing a single classical ticket to make use of the service multiple times[S7]. In contrast the unavailability of long distance quantum communication would disallows them to share a qticket in such a way (i.e. each valid qticket may only be at one place at a time).

S.4.4. The Quantum Credit Card

Having developed a single verification, noise tolerant, non-forgeable token, such as the cv-qticket, it is now possible to examine generalizations to interesting composite protocols. For instance, Gavinsky's proposal[S5] allows for multiple verification rounds to be performed on a single token, while also ensuring that the token can not be split into two independently valid subparts. Such a construction may be seen as a quantum credit card. Indeed, the classical communication which takes place with the issuer (bank) to verify the cv-qticket (via "challenge" questions) may be intentionally publicized to a merchant who needs to be convinced of the card's validity. An alternate possibility is to follow the original interpretation as a quantum cash token where verification is performed by the receiver each time the "money" changes hands.

S.4.5. Excluding eavesdropers

While qtickets do not provide additional advantage against dishonest holder in the scenario of a single verifier quantumness may provide an advantage against eavesdropping and untrusted communication. In order to make online banking more secure, Banks routinely use TANs (transaction authentication numbers) as an additional security measure. The bank sends its client a list of TANs via postal service in addition to an online password which is set up via another channel. Each time a bank transaction is requested online by the client, the bank requests a TAN from the list to guarantee the authenticity of the transaction. An impostor then needs to know both a secret password used by the user and some TANs, thus increasing the difficulty to successfully impersonate a transaction with respect to any single security measure. However, since TANs are classical objects it is conceivable that an eavesdroper may learn them while remaining undetected (imagine an eavesdroper taking xray pictures of the correspondence). This means that with some effort of the eavesdroper the additional security measure becomes ineffective.

This problem can be straightforwardly resolved by using quantum prepare and measure memories. Even if a cv-qticket is sent via an untrusted optical fiber or postal service, the receiver may openly communicate with the issuer and sacrifice some of the received qubits in order to obtain a bound on how much information could have leaked to eavesdroppers. This is precisely the approach taken in QKD to obtain a statistical bound on the information that has leaked out. Gavinsky's Q scheme, allowing multiple verification rounds may be reinterpreted as quantum TAN lists. The holder of a quantum TAN list may verify its validity, and perform a transaction by publicly communicating with the bank. If the quantum TAN list is verified to be legitimate, then the probability of an eavesdroper getting verified by using the leaked information will be negligible (exponentially small). In turn, the cv-qtickets described in the main text and appendix may be used as basic building blocks for such a scheme in the presence of noise.

S.4.6. Combining with classical computational assumptions

The qticket and cv-qticket protocols proposed require the verifiers to have access to secret information (i.e. information which is sufficient to produce additional tokens). This poses a problem for situations where the verifiers can not be trusted with such sensitive information. Ideally, it should be possible to verify the tokens relying exclusively on publicly available information. Seeking to achieve this, Bennet et. al. [S6] made an ingenious proposal based on computational assumptions. We consider a family of such proposals and show that they are not secure.

The proposal of Bennet et. al can be abstractly presented as follows. The mint secretly keeps the solution to a publicly known instance of a computationally hard problem. The problem instance may have been generated by the mint from the solution in the first place. It is then possible for the mint to interactively convince anyone that it has the solution to the prob-

lem without giving away any additional information about the solution. Such a method for convincing is known as a statistical zero knowledge proof (SZKP). For many problems, SZKP can be set up in a *cut and choose* fashion. This is, the mint “cuts” the secret solution into two parts m_1 and m_2 which together allow reconstructing the secret solution but independently provide no useful information.

We provide a simple example for this in the context of graph isomorphism. The mint generates two isomorphic graphs G_1 and G_2 , publishes them but keeps the isomorphism secret. The mint can then proceed as follows to convince someone that it has a proof of $G_1 \equiv G_2$. The mint generates a random graph $G_c \equiv G_1$ (which may be seen as the “cut”) by randomly permuting the vertices in G_1 and offers to provide either the isomorphism proving $G_c \equiv G_1$ or the one for $G_c \equiv G_2$. A verifier then randomly “chooses” which of the two to request, a dishonest prover (lacking a proof of $G_1 \equiv G_2$) would have no more than a 50% chance of being capable to answer correctly. Thus by repeating this procedure n times, a verifier can be $1 - 2^{-n}$ certain of the proof being conveyed. On the other hand, the verifier learns no information about the secret solution $G_1 \equiv G_2$ which it could not have easily obtained independently.

In our language, Bennet et al. go one step further and propose that the mint hardcode such SZKPs into a token composed of a classical part and a quantum state. The holder of such a token would thus have access to a one time SZKP of the problem openly published by the mint. In order to do this, the “cut” is provided classically, whereas the two possible proofs are encoded in a quantum state such that either of them may be extracted by measuring the state but not both. As we will show however, this requirement can not be fulfilled if one allows arbitrary coherent operations to be performed on the quantum tokens (i.e. security against the most general attacks is impossible).

Suppose that we wish to encode two possible messages m_1 and m_2 into a large quantum state such that an adversary may learn either of them with a very high certainty but may not learn both of them. In order to show that this is not possible, we consider the simple scenario where two bits of information are encoded in a quantum state such that either of them can be retrieved by measurement with high precision and show that it is possible (at least in theory) to retrieve both of them simultaneously with high success rate.

Consider a family of quantum states $\rho_{\alpha,\beta}$ used to multiplex the classical bits $\alpha, \beta \in \{0, 1\}$. That the holder of the quantum state can extract either α or β may be expressed by

$$\begin{aligned} \text{Tr}[P_\alpha^a \rho_{\alpha',\beta'}] &\geq (1 - \epsilon) \delta_{\alpha,\alpha'} \\ \text{Tr}[P_\beta^b \rho_{\alpha',\beta'}] &\geq (1 - \epsilon) \delta_{\beta,\beta'} \end{aligned} \quad (S37)$$

where $\{P_\alpha^a\}$ and $\{P_\beta^b\}$ are two projective measurements indexed over α and β respectively (i.e. $P_0^a + P_1^a = P_0^b + P_1^b = \mathbb{1}$). We wish to show that by successively performing both projective measurements both α and β may be obtained with relatively high certainty. Hence it is impossible to multiplex the α and β such that either may be recovered reliably but attempting to measure both remains highly unreliable. The

POVM corresponding to sequential measurement is given by $\hat{P}_{\alpha,\beta} = P_{\alpha}^a P_{\beta}^b P_{\alpha}^a$ and we will show that it is good to order $\sqrt{\epsilon}$

$$\begin{aligned} & \text{Tr}[P_{\alpha}^a P_{\beta}^b P_{\alpha}^a \rho_{\alpha,\beta}] \\ &= \text{Tr}[P_{\beta}^b \rho_{\alpha,\beta}] - \text{Tr}[P_{\beta}^b P_{\alpha}^a \rho_{\alpha,\beta} P_{\alpha}^a] - (\text{Tr}[P_{\beta}^b P_{\alpha}^a \rho_{\alpha,\beta} P_{\alpha}^a] + c.c) \\ &\geq 1 - 2\epsilon - 2\sqrt{\text{Tr}[P_{\beta}^b P_{\alpha}^a \rho_{\alpha,\beta} P_{\alpha}^a] \text{Tr}[\rho_{\alpha,\beta} P_{\alpha}^a]} \\ &\geq 1 - 2\epsilon - 2\sqrt{\epsilon} \end{aligned}$$

(S38)

where we have used the Cauchy-Schwartz inequality to go obtain the second line simplifying further with $P_{\alpha}^a \succ (P_{\alpha}^a)^2$ and $P_{\beta}^b \succ (P_{\beta}^b)^2$. Hence if we make ϵ arbitrarily small, this will also make the probability of extracting both indices arbitrarily close to 1.

- [S1] H. Zhu and B. Englert, *Physical Review A* **84**, 022327 (2011), URL <http://link.aps.org/doi/10.1103/PhysRevA.84.022327>.
- [S2] A. Panconesi and A. Srinivasan, *SIAM Journal on Computing* **26**, 350 (1997), ISSN 00975397.
- [S3] R. Impagliazzo and V. Kabanets, *Tech. Rep.* 072 (2010).
- [S4] R. F. Werner, *Physical Review A* **58**, 1827 (1998).
- [S5] D. Gavinsky, arXiv:1109.0372 (2011).
- [S6] C. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, in *Advances in CryptologyProceedings of Crypto* (1983), vol. 82, pp. 267–275.
- [S7] If the classical ticket is not renewed upon control even communication is unnecessary.